IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-2, Issue-4 E-ISSN: 2347-2693

A Bimodal Biometric Technique Based Enhanced Real-Time ATM System with Intelligence Security Measures

Vithya.T[1*] and Parthiban S2

[1*,2]*Embedded System Technologies, Anna University, India*

www.ijcseonline.org

Received: 17/03/2014 Revised: 28/03/2014 Accepted: 22/04/2014 Published: 30/04/2014

Abstract - In this paper, a real-time embedded multimodal biometric recognition system for authentication on Automated teller machine is being developed. The system is implemented on an embedded platform and equipped with novel multimodal recognition algorithms, so this system is an intelligent security system; it is developed based on a teller machine concept. Wherein, the transaction is successful, If and only if the biometric used is matched and GSM technology is used.

Keyword- Bimodal Biometric, Decision Level Fusion, Finger vein, Iris Recognition, GSM

I. INTRODUCTION

Automated teller machine (ATMs) is a well known human friendly device which is based on a person's individuality for personal and business financial transactions on day to day activities. We all know ATM's that accept our credit/debit card and the PIN number to dispense cash. Biometric ATM's are the latest inventions to help us avoid fraud and duplication. If somebody steals our card and also knows our PIN they can easily withdraw cash from our account. In case of biometric ATM's they cannot. Usually the PIN for bio ATM's is the finger print of the card holder or his eye retina scan etc. These cannot be duplicated and hence they are very safe and secure.

With the development of biometric solutions for the ATMs there is no need to remember PIN numbers. Software vendors are coming up with fusion biometric solutions for the rural masses. Where user's biometric data would be scanned into a special PC with a scanner and the scanned feature is then stored in an encrypted form in a central server. When a customer inserts (or swipes) his card in a biometric enabled ATM, he is prompted to set his feature in the scanner. The transaction along with customer's biometric information is passed on to the switch. The switch verifies the biometric feature with the server, and if successful, requests the banking application to authorize the transaction." Based on the result, the Switch instructs the ATM to complete the transaction.

Benefits of Biometric Supported ATMs 1) Provides strong authentication 2) Can be used instead of a PIN 3) Hidden costs of ATM card management like card personalization, delivery, management, re-issuance, PIN generation, help-desk, and re-issuance can be avoided 4) Ideal for Indian rural masses 5) It is accurate 6) Flexible account access allows clients to access their accounts at their convenience 7) Low operational cost of the ATMs will ultimately reduce TCO.

Multimodal system also provides anti-spooling measures by making it difficult for an intruder to spool multiple biometric traits simultaneously. Fusion of finger vein and Iris extraction is user friendly and well accepted system with better performance.

The rest of the paper is organized as follows: The detailed literature survey is given in section II, overview of the system III, the methodology of proposed model is explained in section IV, and the Fusion methods are shown in section V, the security measures in section VI and finally conclusion discussed in section VII.

II. LITERATURE SURVEY

The comparative performance [1] from three different approaches for multimodal recognition of combined iris and fingerprints: classical sum rule, weighted sum rule, and fuzzy logic method. The scores from the different biometric traits of iris and fingerprint are fused at the matching score and the decision levels. The scores combination approach is used after normalization of both scores using the min-max rule. Our experimental results suggest that the fuzzy logic method for the matching scores combinations at the decision level is the best followed by the classical weighted sum rule and the classical sum rule in order. The performance evaluation of each method is reported in terms of matching time, error rates, and accuracy after doing exhaustive tests on the public CASIA-Iris databases V1 and V2 and the FVC 2004 fingerprint database.

A Europe's first finger-vein biometric ATMs installed in Poland, [2] the finger vein authentication is a new biometric method utilizing the vein patterns inside one's fingers for personal identity verification. Vein patterns are different for each finger and for each person; and as they are hidden underneath the skin's surface, forgery is extremely difficult. These unique aspects of finger vein pattern recognition set it

Corresponding Author: *Vithya.T*
Embedded System Technologies, Anna University, India

apart from previous forms of biometrics and have led to its adoption by the major Japanese financial institutions as their newest security technology. Hitachi developed its original light transmission technology for finger vein biometric authentication. As opposed to light reflection, whereby a captured image is taken from light reflected off the surface of the skin, light transmission captures a vein pattern image from light that passes through the surface of the skin.

A system designed on biometric Strategy (Fingerprint) Measure for Enhancing ATM Security in Indian e-banking System [3] is to develop an embedded system board attached with a finger print scanner module and the entire finger prints will be stored before starts the process. Whenever enrolled persons go to ATM,s the first operation that perform is authentication of the persons and the whatever the operation he wants to perform he can do. We will use 100 finger prints storage capable FPRS scanner. It has a stigma of criminality.

An analyzes on the Iris Biometrics for Embedded Systems has been chosen to be implemented due to the low error rates and the robustness their algorithms provide. Several design alternatives are presented, and their analyses are reported [4] with these results, most of the needs required for the development of an innovative identification product are covered. Results indicate that the architectures proposed herein are faster (up to 20 times), and are capable of obtaining error rates equivalent to those based on computer solutions. Simultaneously, the security and cost for large quantities are also improved. But it requires cooperation from the user.

The demand for simple, convenient, and high security authentication systems [5] for protecting private information's stored in mobile devices has steadily increased with the development of consumer electronics. The personal information's can be protected in the form of biometrics which uses human physiological or behavioral features for personal identification. In this paper, we propose real time finger-vein recognition using image processing. Here we have implemented this system using MATLAB and equipped with finger -vein recognition algorithm.

III. OVERVEIW OF THE SYSTEM

The proposed system consists of three hardware modules:

- Image acquisition module,
- DSP main board,
- Human machine communication module.

The image acquisition module is used to collect finger-vein and iris images. The DSP main board including the DSP chip, memory (flash), and communication port is used to execute the biometric recognition algorithm and communicate with the peripheral device. The human machine communication module (buzzer, relay, LCD or keyboard) is used to display recognition results and receive inputs from users. The system also processes the third person authentication using password techniques if and only if the user allows for the transaction, this acceptance or rejection is carried out by using GSM communication between the user and the system.

The proposed biometric recognition algorithm contains two stages: the enrollment stage and the verification stage. Both stages start with images pre-processing, which includes detection of the region of interest (ROI), image segmentation, alignment, and enhancement.

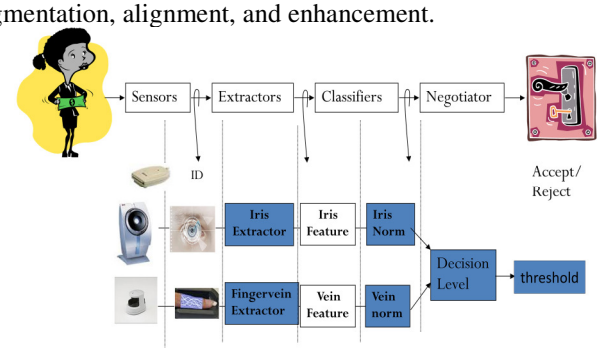

Fig.1. Flow-chart of the proposed recognition algorithm

For the *enrollment stage*, after the pre-processing and the feature extraction step, the finger-vein and iris template fusion value database is built. For the *verification stage,* both the input images fusion value is matched with the corresponding template after its features are extracted. Fig. 1 shows the flow chart of the proposed algorithm.

IV. METHODOLOGY

The proposed system combines two biometric modalities, namely finger vein and iris module.

Finger vein analysis

Advantages:

(1) The vein is hidden inside the body and is mostly invisible to human eyes, so it is difficult to forge or steal. (2) The non-invasive and contactless capture of finger-veins ensures both convenience and hygiene for the user, and is thus more acceptable. (3) The finger-vein pattern can only be taken from a live body.

To develop a finger vein image (Near infra-red image) it is necessary to develop special devices which do not affect the ambient temperature. Usually, finger-vein images can be captured based on Light transmission or Light reflection. To get a better image here we use Light transmission. The modules here we use are: Web Camera by removing IR filter. Light-emitting diode (LED) is used as illumination source for IR light. LED has high permeability and power.

Fig.2: Image acquisition device

As explained in section 3 two stages of biometrics

1. Enrollment Stage:
The enrollment stage is to enroll users to the system. First it takes the finger-vein image from the web-camera. Image segmentation and enhancement process are done by using Image processing technique and the software used here is MATLAB.

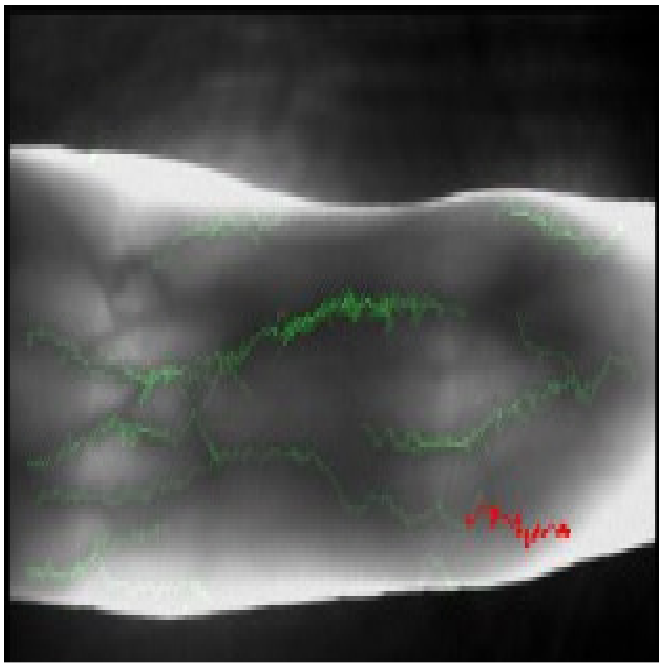

Fig.3: Finger-vein image captured by our device

The finger-vein patterns are extracted by calculating various parameters like vein Width, Length, Position, Pixels and Intersection points of vein. Then they are stored as featured templates. The flowchart is shown below

Verification Stage
The verification stage enables the current user to lock or unlock his system. Like enrolment stage, the verification stage also has to deal with Web camera, MATLAB, database, and PC to store and display the results. This stage will check if the finger vein of the current user is matched with the featured templates or not. The flowchart for this stage is shown below

Image Segmentation and Enhancement
The position of fingers usually varies according to different finger-vein images. So it is necessary to normalize the finger-vein images before feature extraction and matching. When a finger is irradiated by IR rays uniformly, the vein images will look brighter than other parts. The segmented finger-vein image is then enhanced to improve its contrast level. Then the image is resized to 1/4th of the original size. Finally, histogram equalization is used for enhancing the gray level contrast of the image.

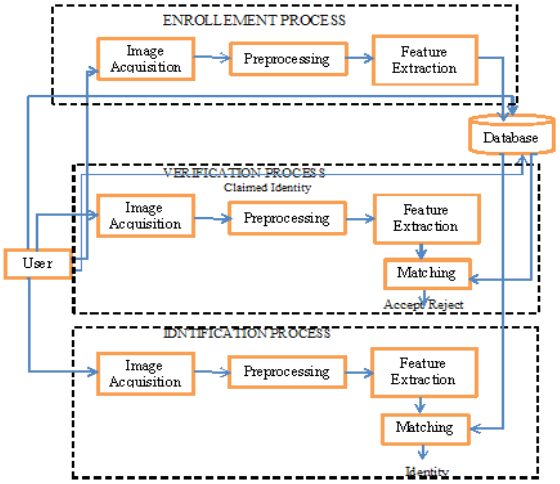

Fig: 4 Biometric System Architecture

Iris extraction analysis
Advantages:
(1)Unique for each person and each eye (2) Well protected and extremely difficult to be modified (3) The identification error rate extremely small and the method is very fast (4) Iris forms during gestation and remains the same for the rest of one's life.

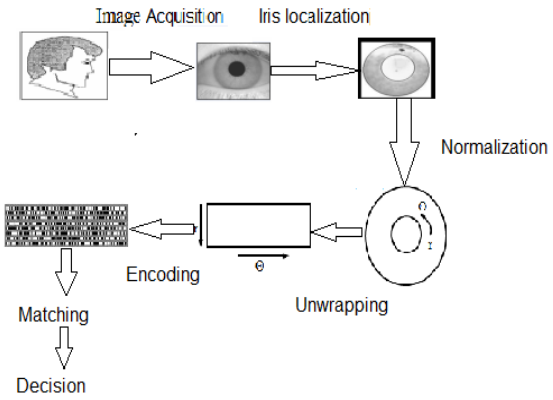

Fig 5: Iris Recognition Process

Step 1: Image Pre-Processing

- Acquisition of images
- Reflection removal using morphology
- The complement of the iris image is taken to make the reflection lighter, the image is then filled with holes to darken the reflections .The complement of the image is taken again to convert the image back to grayscale

I = imcomplement (imfill (imcomplement(I), 'holes'));

Step 2: Iris Segmentation

- Outer and inner iris boundaries localization using Daugman's integro-differential operator

- The operator finds the maximum pixel intensity value change (J) by searching the image within the defined radius parameters with a circular integral centered on the point (x0, y0), with radius r of the radial derivate of the original image blurred with a Gaussian kernel G. J, in this case corresponds to the iris-sclera(white) boundary since the pixel intensity change is so great between those regions
-

$$J(r, x0, y0) = G_{\sigma}(r) * (d/dr) \int_{r, x0, y0} (I(x,y)/2\pi r)\, ds$$

$$G_{\sigma}(r) = (1/(\sigma \sqrt{2\pi}))exp(-r^2 / 2\sigma^2)$$

Where,

x_0 , y_0 , r -the center and radius of coarse circle (for each of pupil and iris).

$G_{\sigma}(r)$ -Gaussian functions

$r\,\Delta$ -the radius range

$I(x, y)$ - the original iris image

$G_{\sigma}(r)$ -is a smoothing function

- Occlusions removal using Linear Hough Transform and thresholding

Step 3: Iris Region Normalization

- Using Daugman's Rubber Sheet model maps the coordinates of each Cartesian point from the segmented iris region to polar coordinates (r,θ) where r ranges from 0 to 1 and θ ranges from 0 2π

Step 4: Iris Recognition

- Feature encoding was implemented by convolving the normalized iris pattern with 1D Log-Gaber wavelet.2D normalized patterns are broken up into a number of 1D signal. Each row corresponds to a circular ring on the iris region. The angular direction is taken rather than the radial one, which corresponds to columns of normalized pattern. The features are extracted in codes of 0 and 1.

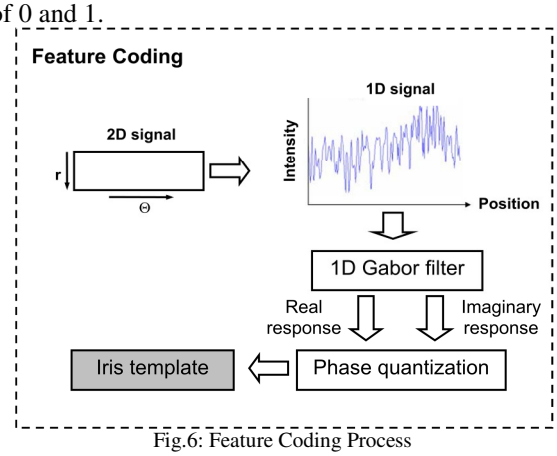

Fig.6: Feature Coding Process

- Feature Matching using the Hamming Distance As a result, a decision can be made in the matching step.

Last, an accept or reject decision is made on the test pattern x using a threshold X, i.e.

Result (x) = accept, if output ≥ X

Reject, if otherwise

V. FUSION IN BIMODAL BIOMETRIC SYSTEMS

A Mechanism that can combine the classification results from each biometric channel is called as biometric fusion. We need to design this fusion. Multimodal biometric fusion combines measurements from different biometric traits to enhance the strengths. Fusion methods are of different types (i.e.) matching score, rank and decision level has been theoretically studied.

Various levels of fusion are: Sensor level, feature level, matching score level and decision level. At the stage of sensor level fusion, multiple biometric traits are taken from different sensors and combined as one composite trait. In feature level fusion, feature vectors of the all processed multi biometrics collected and combined as one. In ***decision level fusion***, every biometric classified independently and finally all it outputs are combined together. In matching score level fusion, matching score of individual modality is derived and fusion as a single matching score.

Fusion at the Decision Level

In a multi biometric system, fusion is carried out at this level when only the decisions output by the individual biometric matchers are available. Here, a separate authentication decision is computed for each biometric trait (i.e., accept or reject in a verification system, or the identity of a user in an identification system) which is then combined to result in a final vote. Different strategies are available to combine the distinct decisions of individual modality to a final authentication decision. The resulting feature vectors from each sensor need to be classified into two classes- reject or accept. Afterwards a majority vote scheme can be used to make a final decision. They are majority voting technique, Boolean conjunctions, AND rule, OR rule, Bayesian decision fusion, the Dempster-Shafer theory of evidence and behavior knowledge space. Fusion at this level is considered to be rigid compared to the other fusion schemes due to the availability of limited information.

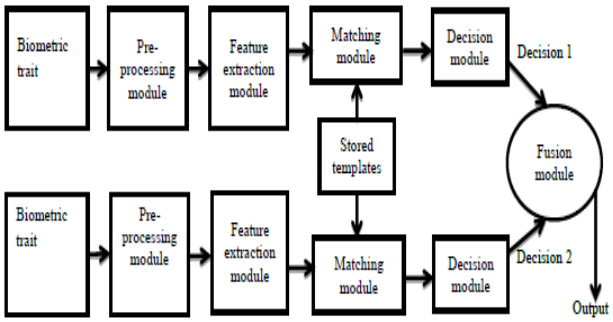

Fig. 7: Fusion at the Decision Level

VI. SECURITY MEASURES OF THE PROPOSED SYSTEM

The proposed system is developed to provide the two way authentication for an individual through biometric and the third person indirect method of authentication using the password technique.

The two way authentication in ATM

- Password based
- Finger vein + Iris based (Fusion)

A Direct transaction method is proposed if the user is present as an individual in the ATM for transaction were he/she can go for the bimodal biometric way of authentication and after processing a message with the transaction details is received to the user mobile through the GSM communication module.

Otherwise in case of emergency the user unavailable to go to the ATM he/ she can undergo an indirect transaction through the third person without providing any PIN or password to the third person that is without any knowledge about the users banking details. The third person carries only the ATM card along with him/her. When starting with the process the system accepts the card and transmit a message to the user asking for acceptance, (showing the *processing*….. to the third person) the user on the other hand replies with the acceptance if and only if the third person is the one he/she has sent, otherwise he can reply with rejection message.

If the user sends acceptance reply then it is considered as an authorized person so the system further processes for withdrawal/transaction and also sends the details to the user mobile. Or if the user sends the rejection reply than it is the unauthorized person and three trails are provided if all the three are rejected then an message saying about the unauthorized transaction is sent to the user, nearby police and the bank, at once the buzzer is put ON automatically to make the nearby people alert, then the door is locked until the police arrives and the transaction is cancelled.

VII. CONCLUSION

Most of the banking applications will be running basis on biometrics and it is the only way to guarantee the presence of the customer when a transaction is made. For instance, multimodal biometric systems have been proven to be very effective in protecting information and resources in banking applications. Multibiometric systems, which integrate information from multiple biometric traits, are gaining popularity because they are able to overcome limitations of unimodal biometrics. Until recently, most research in multi-modal biometrics has concentrated on combining data at decision or score levels.

REFERENCES

[1]. Houda Benaliouche andMohamed Touahria , "*Comparative Study of Multimodal Biometric Recognition by Fusion of Iris and Fingerprint*", Computer Science Department, University of Ferhat Abbas S´etif 1, P^ole 2 - El Bez, 19000 S´etif, Algeria Received 28 August 2013;

[2]. Yanagawa,A.K. Aoki,Y and Ohyama,I,"An *Europe's first finger-vein biometric ATMs installed*" ,Proc. IEEE International Symposium on Intelligent Control in Poland July 2011.

[3]. Sri Shimal Das and Smt. Jhunu Debbarma "*Designing a Biometric Strategy (Fingerprint) Measure for Enhancing ATM Security in Indian e-banking System*" Volume 1 No. 5, September 2011 ISSN-2223-4985 IJICT ,2011.

[4]. Sanchez-Reillo,R.Fernandez-Saavedra,B. & Liu-Jimenez,J,"*Iris Biometrics for Embedded Systems*" Very Large Scale Integration (VLSI) Systems, IEEE Transactions on (Volume:19, Issue:2) Biometrics Compendium, IEEE Trans, Feb. 2009

[5]. Vanathi G, Nigarihaa R, Uma Maheswari G & Sujitha R "*Real Time Recognition System Using Finger-Vein* " Electronics and Communication Engineering, Avinashilingam, University Coimbatore, India

[6]. "Optimized Daugman's Algorithm for Iris Localization" Dr. Mohamed A. Hebaishy National Authority for Remote Sensing and Space Science Gozif Titp St., Elnozha Elgididah. Egypt (11769).

[7]. Anil K. Jain,Michigan State University and Karthik Nandakumar Institute for Infocomm Research, Singapore "Biometric Authentication: System Security and User Privacy"

[8]. Jammi Ashok, VAKA SHIVASHANKAR and P.V.G.S.MUDIRAJ, "An Overview of Biometrics" (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 07, 2010, 2402-2408

AUTHORS PROFILE

T.VITHYA received her B. Tech degree in Electronics and Communication engineering from the Department of Electronic & Communication, Pondicherry University and M.E degree in Embedded System Technologies from the Department of Electronic & Communication, Anna University. Her area of interest includes Embedded system and Image Processing.

PARTHIBAN.S received her B.E degree in Electronics and Communication engineering from the Department of Electronic & Communication, Anna University and M.E degree in Embedded System Technologies from the Department of Electronic & Communication, SRM University.
His area of interest includes Embedded system.